## Fail2Ban

written by archi | 15 kwietnia 2021

Laboratorium ma na celu wprowadzenie mechanizmów bezpieczeństwa do systemów sieciowych. W tym przypadku zostanie uruchomione oprogramowanie przeznaczone do analizowaniu dzienników zdarzeń systemu i aplikacji na nim działających w celu prowadzenia polityki bezpieczeństwa. Ideą działania pakietu Fail2Ban jest aktywne wpływanie na system zapory ogniowej (firewall) poprzez blokowanie hostów atakujących lub prowadzących nie właściwe działania. Takie działania mogą wynikać np. z prób logowania się na obce konta.

1. Aktualizuj bazę dostępnego oprogramowania w systemie

```
apt-get update
```

2. Zainstaluj pakiet "fail2ban"

```
apt-get install fail2ban
```

3. W katalogu "/etc/fail2ban" zostały zgromadzone pliki konfiguracyjne tego pakietu.

```
fail2ban
/ action.d
/ abuseipdb.conf
/ [...]
/ -xarf-login-attack.conf
/ /fail2ban.d
/ /filter.d
/ /ignorecommands
| /ignorecommands
| ] [...]
| _ zoneminder.conf
```

```
/jail.d
/ jail.d
/ defaults-debian.conf
/ fail2ban.conf
/ jail.conf
/ paths-arch.conf
/ paths-common.conf
/ paths-debian.conf
/ paths-opensuse.conf
```

4. Należy włączyć sprawdzanie dla "sshd", "webmin-auth" w pliku "/etc/fail2ban/jail.d/defaults-debian.conf"



5. W pliku "/etc/fail2ban/jail.conf" należy zmienić wartości domyślne dla: bantime = 1m, findtime = 1m i maxretry = 3



W tym samym pliku podane są domyślnie parametry dla kolejnych właczonych wcześniej więzień (jail)

```
[sshd]
port = ssh
logpath = %(sshd_log)s
[sshd-ddos]
# This jail corresponds to the standard configuration in Fail2ban.
# The mail-whois action send a notification e-mail with a whois request
# in the body.
port = ssh
logpath = %(sshd_log)s
```

```
[webmin-auth]
port = 10000
logpath = %(syslog_authpriv)s
```

6. Po wprowadzeniu wszystkich zmian restartujemy usługę:

```
services fail2ban restart
```

7. Sprawdzimy czy usługa działa poprawnie:

fail2ban-client

8. Wykonamy test sprawdzający czy więzienie dla Webmin-Auth działa:

- wykonaj polecenie dla sprawdzenia wpisów

fail2ban-client status

- w wyniku powinieneś zobaczyć odpowiedź systemu

Status |- Number of jail: 2 `- Jail list: sshd, webmin-auth

- sprawdzimy wpisy w Firewall

iptables -L -n

| Chain INPUT | hain INPUT (policy ACCEPT) |             |  |  |  |  |
|-------------|----------------------------|-------------|--|--|--|--|
| target      | prot opt source            | destination |  |  |  |  |
| Chain FORWA | RD (policy ACCEPT)         |             |  |  |  |  |
| target      | prot opt source            | destination |  |  |  |  |
| Chain OUTPU | T (policy ACCEPT)          |             |  |  |  |  |
| target      | prot opt source            | destination |  |  |  |  |

## Sprawdzenie możesz również wykonać poprzez Webmin

|                                     | Ø               |   |  |                                 |                                |   |  |
|-------------------------------------|-----------------|---|--|---------------------------------|--------------------------------|---|--|
| Webmin                              | Daebboard       |   | 50   | olid-pop3d                      | No                             |   |  |
| webmin                              | Dashbuaru       |   | ex   | am                              | No                             |   |  |
|                                     |                 |   | ex   | cim-spam                        | No                             |   |  |
| Search                              |                 |   | ke   | erio                            | No                             |   |  |
|                                     |                 |   | 0  | ourier-auth                     | No                             |   |  |
| Webmin                              |                 |   | po   | ostfix-sasl                     | No                             | postfix[mode=auth]  |  |
|                                     |                 |   | pe   | erdition                        | No                             |   |  |
| System                              |                 |   | sq   | quirrelmail                     | No                             |   |  |
|                                     |                 |   | су   | yrus-imap                       | No                             |   |  |
| Servers                             |                 |   | UV   | wimap-auth                      | No                             |   |  |
| 🗙 Tools                             |                 |   | na   | amed-refused                    | No                             |   |  |
|                                     |                 |   | ns   | sd                              | No                             |   | %(banaction)s   %(banaction)s  |
| S Networking                        |                 |   | as   | sterisk                         | No                             |   | %(banaction)s   %(banaction)s   %(mta)s-whois  |
| Bandwidth Mo                        |                 |   | fre  | eeswitch                        | No                             |   | %(banaction)s   %(banaction)s   %(mta)s-whois  |
| College Inter                       | -i D-tt         |   | zn   | nc-adminlog                     | No                             |   |  |
| <ul> <li>Palizban intru</li> </ul>  | aion Detector   |   | m  | vsgld-auth                      | No                             |   |  |
| <ul> <li>Linux Firewall</li> </ul>  |                 |   | m  | ongodb-auth                     | No                             |   |  |
| <ul> <li>Linux IPv6 Fire</li> </ul> |                 |   | re   | cidive                          | No                             |   |  |
| Network Confi                       |                 |   | Da   | am-generic                      | No                             |   |  |
| All officers and                    |                 |   | xir  | netd-fail                       | No                             |   |  |
| <ul> <li>NIS Client and</li> </ul>  |                 |   | st   | tunnel                          | No                             |   |  |
| <ul> <li>TCP Wrappers</li> </ul>    |                 |   | ei   | abberd-auth                     | No                             |   |  |
| G Hardware                          |                 |   | 0  | ounter-strike                   | No                             |   | %(banaction)s I %(banaction)s  |
| -                                   |                 |   | bit  | itwarden                        | No                             |   | -demonstration (and a second sec |
| Cluster                             |                 |   | Ce   | entreon                         | No                             |   |  |
| the standard black                  |                 |   | na   | agios                           | No                             |   |  |
| n+ Un-used Modu                     | uies •          |   | or   | racleims                        | No                             |   |  |
| C Refresh Modu                      |                 |   | di   | irectadmin                      | No                             |   |  |
|                                     |                 |   | 00   | ortsentry                       | No                             |   |  |
|                                     |                 |   | D P  | ass2allow-ftp                   | No                             | anache-nass[knocking.ut]="%/knocking.ut]s"]                                   | %(action )s  |
|                                     |                 |   | m  | urmur                           | No                             | abreate beenfunceaurillion affeneeurillion ye 1                               | %(banaction)s I %(banaction)s  |
| 14 2 2 1                            | er er 20 user 📭 |   | sc   | reensharingd                    | No                             |   |  |
|                                     |                 |   | ha   | aproxy-http-auth                | No                             |   |  |
|                                     |                 |   | sla  | and                             | No                             |   |  |
|                                     |                 |   | de   | omino-smtp                      | No                             |   |  |
|                                     |                 |   | ph   | homvadmin-syslog                | No                             |   |  |
|                                     |                 |   | 20   | oneminder                       | No                             |   |  |
|                                     |                 |   | tra  | aefik-auth                      | No                             |   |  |
|                                     |                 | _   | 88   | shd                             | Yes                            |   |  |
|                                     |                 |   | W  | ebmin-auth                      | Yes                            |   |  |
|                                     |                 |   |  |                                 |                                |   |  |
|                                     |                 |   | Select   | t all 🕑 Invert selection 🕀 Ad   | id a new jail                  |   |  |
|                                     |                 |   | O Dele   | ete Selected Jails              |                                |   |  |
|                                     |                 | -   |  |                                 |                                |   |  |
|                                     |                 |   |  |                                 |                                |   |  |
|                                     |                 |   |  |                                 |                                |   |  |
|                                     |                 |   | Edit Ja  | ail Defaults Edit default setti | ngs and limits that apply to a | II the jails listed above, such as the number of required matches and the tir | ne to ban an IP for.   |
|                                     |                 |   |  |                                 |                                |   |  |
|                                     |                 | A CONTRACTOR OF |  |                                 |                                |   |  |
|                                     |                 |   |  |                                 |                                |   |  |
|                                     |                 |   | D de la companya de la<br>companya de la companya d | and a second star in stars      |                                |   |  |

informacje w systemie pojawią się dopiero po wykonaniu lub pojawieniu się
 blokad po nieuprawnionych działaniach w systemie

| root@linux:~# iptables -L -n<br>Chain INPUT (policy ACCEPT)<br>target prot opt source<br>f2b-webmin-auth tcp 0.0.0.0/0 | destination<br>0.0.0.0/0              | multiport dports 10000            |
|--|---------------------------------------|-----------------------------------|
| Chain FORWARD (policy ACCEPT)<br>target prot opt source  | destination                           |                                   |
| Chain OUTPUT (policy ACCEPT)<br>target prot opt source   | destination                           |                                   |
| Chain f2b-webmin-auth (1 references)<br>target prot opt source<br>REJECT all 192.168.99.129<br>RETURN all 0.0.0.0/0    | destination<br>0.0.0.0/0<br>0.0.0.0/0 | reject-with icmp-port-unreachable |

- zaloguj się na stronie "https://192.168.x.x:10000/" do konsoli

Webmin w sposób prawidłowy oraz następnie wykonaj 3x błędne logowanie

| You must enter a username and password to login to the server on |  |  |  |  |
|--|--|--|--|--|
| Lusername  |  |  |  |  |
| Password   |  |  |  |  |
| Remember me  |  |  |  |  |
| ➡ Sign in  |  |  |  |  |
|  |  |  |  |  |

 - gdy zalogujemy się niepoprawnie po raz trzeci (3) to nastąpi zablokowanie dostępu dla adresu IP z którego się logowaliśmy i dostęp do strony Webmin będzie zablokowany na ustawiony wcześniej czas 60s.

| Chain f2k | -sshd-dda | os (1 references)   |             |                                   |
|-----------|-----------|---------------------|-------------|-----------------------------------|
| target    | prot op   | ot source           | destination |                                   |
| RETURN    | all       | - 0.0.0.0/0         | 0.0.0/0     |                                   |
|           |           |                     |             |                                   |
| Chain f2k | -webmin-a | auth (1 references) |             |                                   |
| target    | prot or   | nt source           | destination |                                   |
| REJECT    | all       | 82.145.93.80        | 0.0.0/0     | reject-with icmp-port-unreachable |
| RETURN    | all       | - 0.0.0.0/0         | 0.0.0/0     |                                   |
|           |           |                     |             |                                   |

Jeśli uzyskasz taki efekt to usługa została skonfigurowana poprawnie...